IN THE ABSTRACT:

Replace the abstract originally provided on the cover sheet of the PCT application with the new abstract as follows. A new abstract numbered page 22 is enclosed for the last page of the application following the claims.

ABSTRACT OF THE DISCLOSURE

A combinatorial key-dependent network suitable for the encryption/decryption of data on buses and in memories of data-processing devices, has a number of layers, where each layer has of a number of elementary building blocks operating on very small block sizes. A generic building block acts on a small number of input data bits, which are divided into two groups of m and n bits, respectively. The m input bits, which are passed to the output intact, are used to select k out of 2^mk key bits by a multiplexer circuit; the k bits are then used to select an (nxn)-bit reversible transformation acting on the remaining n input bits to produce the corresponding n output bits. The total number of the key bits in the building block is thus 2^mk, which can easily he made larger that m+n. An inverse building block is the same except that the reversible transformations are replaced by their inverses.

ABSTRACT OF THE DISCLOSURE

A combinatorial key-dependent network suitable for the encryption/decryption of data on buses and in memories of data-processing devices, has a number of layers, where each layer has a number of elementary building blocks operating on very small block sizes. A generic building block acts on a small number of input data bits, which are divided into two groups of m and n bits, respectively. The m input bits, which are passed to the output intact, are used to select k out of 2^mk key bits by a multiplexer circuit; the k bits are then used to select an (nxn)-bit reversible transformation acting on the remaining n input bits to produce the corresponding n output bits. The total number of the key bits in the building block is thus 2^mk, which can easily he made larger that m+n. An inverse building block is the same except that the reversible transformations are replaced by their inverses.